ENSAYO SOBRE SEGURIDAD FISICA Y CONTINUIDAD DEL NEGOCIO

JUAN ANTONIO GONZALEZ RODRIGUEZ

WILFREDO VELEZ CEDEÑO

UNIVERSIDAD MILITAR NUEVA GRANADA

UNIVERSIDAD SAN BUENAVENTURA

ESPECIALIZACION EN ADMINISTRACION DE SEGURIDAD

CALI

2012- 06- 15

LA SEGURIDAD FISICA Y SUS COMPONENTES COMO PARTE FUNDAMENTAL EN LA CONTINUIDAD DE LOS NEGOCIOS

JUAN ANTONIO GONZALEZ RODRIGUEZ

WILFREDO VELEZ CEDEÑO

LUIS GABRIEL FERRER

MG EN EDUCACION EES

ESPECIALIZACION EN ADMINISTRACION DE SEGURIDAD

CALI

2012- 06- 15

TABLA DE CONTENIDO.

Pág.

RESUMEN

La seguridad física tiene un valor fundamental en las organizaciones y requiere de mucha atención por parte de las altas gerencias, buscando la protección del personal, los bienes, instalaciones y los procesos, mediante la generación de estrategias organizacionales, de tal forma que se cuente con un diseño de seguridad efectivo, fundamentado en capas de seguridad, determinando en cada una de ellas la detección, el retardo y la respuesta logrando tener los riesgos plenamente identificados y controlados.

La seguridad física, toma parte activa en la continuidad de los negocios, siendo este ultimo el tema de mayor relevancia en las organizaciones en la gestión de riesgos, para permitir que la compañía perdure en el tiempo, ante la materialización de los riesgos.

Con la puesta en marcha de un plan de continuidad del negocio, las compañías estarán mejor preparadas para afrontar situaciones adversas que podrían llegar inclusive a desaparecer una organización, aquí la importancia que tiene el trabajar mediante la prevención y no en la reacción.

INTRODUCCION

La seguridad física como parte fundamental en la continuidad de los negocios, debe ser vista como una actividad primordial para permitir que las compañías puedan tener capacidad de prevención, acción y reacción frente a una situación adversa, en la cual se exponga la integridad de las personas, el patrimonio representado en activos e instalaciones, y en los procesos.

En la aplicación profesional de la seguridad, se encuentran diferentes conceptos y aplicaciones; por lo cual la importancia de poder conocer, analizar y desarrollar un correcto plan de continuidad de negocios que permita de manera estratégica a una compañía, colocar en práctica los mejores conocimientos y experiencias en seguridad; siendo esta situación una de las principales razones por la cual se hace el presente ensayo en la seguridad física como parte fundamental en la continuidad de los negocios, permitiendo ampliar el concepto en forma profesional.

LA SEGURIDAD FISICA Y SUS COMPONENTES COMO PARTE FUNDAMENTAL EN LA CONTINUIDAD DE LOS NEGOCIOS.

El Diseño y evaluación de los sistemas de protección física

De acuerdo al autor Mary Lynn García "Un sistema de protección física (PPF) integra personas, procedimientos, y equipo para la protección de bienes o instalaciones contra el robo, sabotaje u otros ataques humanos mal intencionados. El diseño de un PPF requiere de un sistema metódico por el cual el diseñador pesa los objetivos del PPF contra los recursos disponibles y luego evalúa el diseño propuesto para determinar su eficacia para alcanzarlos. Sin esta evaluación cuidadosa, el PPF podría perder recursos valiosos en protección innecesaria y lo que es peor, no proveer la debida protección en puntos críticos de servicios. Por ejemplo, sería imprudente proteger las instalaciones de un empleado de una cafetería con el mismo nivel de protección con el área central de cómputo. De manera similar la máxima seguridad en la entrada principal de una instalación sería innecesario si la entrada fuese también posible a través de una cafetería desprotegida. Cada instalación es única, incluso si se desarrollan actividades semejantes generalmente, de ahí que este alcance sistemático permita flexibilidad en la aplicación de herramientas de seguridad que direccionen las condiciones locales" (Mary Lynn García. 2008. Pág. 14).

Es fundamental en el diseño de un sistema de protección física, hacer una adecuada evaluación de todas las vulnerabilidades y amenazas que se pueden encontrar presentes en la operación o entorno de una organización, logrando de esta manera identificar los riesgos que más le pueden afectar en la continuidad de sus negocios; siendo esta razón por la cual el especialista

en seguridad debe tener un conocimiento integral en la prevención de riesgos, priorizando a su vez cada uno de ellos, de acuerdo a la cuantificación de los mismos.

La evaluación de riesgos es un ejercicio cuidadoso y el cual se soporta en el conocimiento en diversas metodologías de riesgos, fundamentalmente en los términos de amenaza, riesgo y vulnerabilidad, siendo estos los factores primordiales de identificación para poder determinar los niveles de criticidad de riesgos y el tratamiento que se debe cumplir para poder minimizar y estabilizar la operación de una organización, pensando en su continuidad en el tiempo.

La seguridad en la industria

Según afirma el autor "La seguridad en la industria es un negocio de muchos miles de millones de dólares. Cada década parece traer una incrementada necesidad de los servicios de seguridad. El crimen en las calles, el terrorismo, el crimen de la tercera oleada y otros mas, traen consigo una tremenda demanda de protección a las personas y a medios" (Philip p. purpura.2002).

La participación de la seguridad en el mercado mundial, cada vez es más fuerte y competitiva, es por ello que se puede evidenciar en el ingreso de empresas multinacionales en los últimos años al mercado nacional, con músculos financieros muy fuertes, lo que hace que las empresas nacionales deban competir en servicio, calidad, y conocimiento en riesgos basados en muchos casos en la experiencias que afronta el país.

Es así como toma cada vez más importancia la profesionalización de los encargados de manejar la seguridad en las organizaciones, a tal punto que la tendencia es en el nivel estratégico de la seguridad, que existan gerencias en riesgos, quienes a su vez deberán tener unas competencias en riesgos y continuidad de negocios, para poder dar soporte a las necesidades de la empresa y el mercado, teniendo pleno conocimiento de las amenazas del entorno donde se encuentre ubicada la compañía, vulnerabilidades de las instalaciones, los procesos, las personas; pleno conocimiento en temas de seguridad física, seguridad electrónica, seguridad de personal, informática e información, manejo de emergencias, continuidad de los negocios, entre otros temas inherentes a la gestión de riesgos.

El mercado internacional requiere cubrir la alta demanda de los servicios en seguridad, con personal cada vez más competente, con conocimientos integrales en riesgos.

Es de esta manera como la gestión de riesgos, basada en normas y estándares internacionales, se debe definir en las compañías, desde la misma política, involucrando a todo el personal en la prevención de las perdidas, lo cual puede afectar a las personas, bienes, instalaciones y procesos

Valoración del riesgo en la seguridad

Según la norma ISO 28000, "La organización establecerá y mantendrá procedimientos para la identificación continua y valoración de las amenazas de seguridad y amenazas relacionadas con el manejo de seguridad y riesgos, y la identificación e implementación de medidas de control administrativas necesarias. Amenazas de seguridad y riesgo de identificación,

valoración y métodos de control deberían, como mínimo, ser apropiadas a la naturaleza y escala de las operaciones. Esta valoración considerará la probabilidad de un evento y de todas sus consecuencias que incluirá:

a) Amenazas y riesgos de fallas físicas, como pérdida funcional, daño incidental, daño malicioso, terrorista ó acción criminal;
b) Amenazas y riesgos operativos, incluyendo el control de la seguridad, factores humanos y otras actividades que afectan el funcionamiento, condición o seguridad de la organización.
c) Eventos ambientales naturales (tormenta, inundación, etc.), que pueden inutilizar las medidas de seguridad y equipos no efectivos.
d) Factores ajenos al control de la organización, como fallas en equipos suministrados externamente y servicios;
e) Amenazas y riesgos del tenedor de apuestas como fallas para cumplir con los requerimientos Reguladores o daño a la reputación ó marca;
f) Diseño e instalación de equipo de seguridad incluyendo reemplazo mantenimiento, etc.
g) Información y administración de datos y comunicaciones;
h) Una amenaza a la continuidad de las operaciones." (Norma ISO 28000 – 2007).

Con la implementación de esta norma, se generan mayores controles y toma mayor fuerza los sistemas de gestión en seguridad, y especialmente en la cadena de suministros, en la cual el alcance ya no se limita a la seguridad de las instalaciones, si no que por el contrario se deben identificar todos los agentes que intervienen en a lo largo y ancho de la cadena logística, evaluando sus amenazas, riesgos, vulnerabilidades, permitiéndole a su vez mejorar sus tiempos en envíos de mercancía a otros destinos y en especial de cierto modo garantizar que mediante la

implementaciones de estos sistemas de gestión se adoptan medidas, basados en procesos y procedimientos, para minimizar el riesgo y controlar la operación de tal forma que la continuidad de los negocios no se vea afectada al asumir riesgos que al no ser identificados puedan cambiar con facilidad de un nivel a otro (después de evaluar cuantitativamente los riesgos), y afectar toda una compañía.

Para reducir los riesgos en las organizaciones se requiere de una excelente evaluación de los factores de riesgo, y por consiguiente un adecuado tratamiento de los mismos:

Transferir, asumir, reducir, disgregar, evitar; donde se colocan en práctica todos los conocimientos en riesgos, mediante la aplicación de planes de acción, donde se involucren las personas en todos los niveles de las organizaciones, dando cumplimiento a las acciones resultantes, en los planes de intervención de riesgos.

Importancia del análisis de riesgos

Según el texto del autor "Es importante considerar que factores como el control de variables ambientales, tecnologías de control de acceso, y sistemas de CCTV, permiten implementar los controles. Esto controles deben ser el resultado de análisis de riesgo, en donde se determinan las prioridades de cada uno de los elementos anteriormente mencionados" (http://www.sisteseg.com/fisica.html).

Es importante resaltar como el análisis de riesgos es la parte fundamental para lograr identificar los principales riesgos que pueden afectar una organización o persona, donde en

muchas ocasiones no se hace un efectivo análisis, y quedan amenazas que al no ser identificadas pueden materializar cuantiosas pérdidas materiales e inclusive en la vida misma.

El control en las variables ambientales, tecnologías de control de acceso y sistemas de CCTV, son factores fundamentales a considerar en el análisis de riesgos y en el estudio de seguridad, siendo este ultimo donde se requiere de mayor conocimiento y haber definido una metodología que permita cualificar y cuantificar cada uno de los riesgos y de esta manera priorizarlos y poder dar tratamiento a los mismos.

Especialmente en el control de acceso, se deben definir los procedimientos para el ingreso y retiro de personal y activos de la compañía, donde claramente desde la política de seguridad y gestión de la organización deben estar socializadas para que no generen diferencias o molestias en el personal, pensando en que la seguridad no debe ir en contravía con la producción o el core del negocio.

En el modelo de seguridad actual, las herramientas tecnologías tienen cada vez más fuerza, es así como el CCTV, es uno de los elementos fundamentales en la seguridad, apoyando a la gestión en seguridad física en sus actividades de control, pero lastimosamente en algunas organizaciones solamente se tiene como parte fundamental en algunas investigaciones realizando trazabilidad a las actividades que se puedan reportar, debido a que no se cuenta con personal que monitoree en tiempo real los eventos que se están presentando, y solamente se hace una inversión en tecnología, desaprovechando una excelente herramienta que disuade y permite minimizar los riesgos en la organización.

En el diseño de seguridad; la Detección, Retardo y Respuesta

De acuerdo al texto del autor “A pesar de que se invierte miles y en ocasiones millones de dólares en equipo de tecnología de punta para lograr los objetivos económicos que se propone una empresa, actualmente nos encontramos con que muchas organizaciones sufren de incidentes en donde se viola la seguridad física de sus instalaciones por terceros e inclusive por personal interno, esto posiblemente se debe, a que la seguridad física es en muchas ocasiones tomada como un elemento de "menor prioridad ", sea por iniciativa corporativa o por omisión.
Lo que muchos directivos obvian es que la seguridad física describe las medidas que previenen o detienen a intrusos antes de acceder a una instalación, recurso o información almacenada en medios físicos, los cuales pueden ser tan simples como una puerta con seguro, o tan elaborados como múltiples capas de seguridad de guardias armados.

Para estos problemas relacionados con la seguridad en las empresas, la "ingeniería de seguridad", la ciencia encargada de estudiar los aspectos relacionados a la seguridad física, ha identificado tres elementos clave para la seguridad física. El primero, al que llamamos en su conjunto "obstáculos" frustra a atacantes triviales y retarda a los más peligrosos. El segundo, es todo el conjunto de alarmas, iluminación de seguridad, patrullas de guardias de seguridad o controles de circuito cerrado, que facilita y permite que los intrusos sean detectados. Finalmente, el tercer elemento clave es la respuesta para repeler, capturar o frustrar a los atacantes cuando estos hayan penetrado. ([http://www.monografias.com/] boletín 27 Universidad EAFIT. Medellín).

El modelo de seguridad mediante la detección, el retardo y la respuesta, es la mejor manera de efectuar un diseño que permita evaluar los tiempos que se tienen como seguridad frente a una posible intrusión, por tal razón en el evento en cual el diseño de seguridad, el tiempo de intrusión sea menor a la sumatoria de la detección, retardo y respuesta, podremos inferir que el diseño no es efectivo.

Las capas de seguridad que se modelan en un diseño de seguridad, (exterior, intermedia, interior), permiten que se pueda ubicar de acuerdo a las condiciones de estructura de las instalaciones, entorno, ubicación geográfica, los niveles de detección, retardo y respuesta, donde como ya se había manifestado debe estar en medición a los tiempos de intrusión, para que sea dicho tiempo mucho mayor y de esta manera poder minimizar el riesgo y controlarlo mediante la gestión integral de los riesgos.

El pensamiento en la gestión de riesgos, debe estar enfocada a realizar mediciones y simulaciones de las posibles eventos que se puedan materializar, siendo de esta manera la forma en la cual las organizaciones podrán estar preparadas para afrontar un evento adverso, e inclusive ir preparando su continuidad del negocio, siendo este un tema fundamental en la gestión de riesgos y que requiere de toda la atención de las organizaciones, existiendo aquella frase de que riesgo que no se conozca o identifique es riesgo que se asume, y el riesgo asumido es una posible pérdida potencial. La gestión integral de riesgos toma fuerza en las organizaciones cada vez más, debido a los cambios y mayor conocimiento que adquieren las posibles amenazas para las organizaciones, es allí donde la gerencia en gestión de riesgos se debe definir y sustentar ante las diferentes gerencias y desde allí, realizar actividades de capacitación, sensibilización, control, tanto para el personal interno como para todos los grupos de interés, (comunidad, proveedores,

estado, cliente externo, medio ambiente), generando protocolos o procedimientos efectivos que contribuyan con el pleno desarrollo organizacional en cuanto al Core del negocio, permitiendo que la empresa se dedique a su razón natural del negocio y la seguridad sea el soporte eficiente a todos los procesos brindando bienestar y tranquilidad a todo el personal de la organización.

La seguridad física en los centros de cómputo

Según lo manifiesta el autor “Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"(1). Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos” ((1) HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000. http://www.kriptopolis.org).

Parte fundamental en seguridad de las organizaciones es la planeación y ejecución de la seguridad física en las áreas de computo, o áreas donde se guarde información de tipo confidencial y la cual en manos inescrupulosas podría ser utilizada en contra de los intereses de la compañía; es este tipo de información inclusive se tiene información estratégica, la cual al estar en manos de la competencia, generaría un debilidad competitiva.

La aplicación de barreras físicas y procedimientos de control, deben estar definidas por un profesional en gestión de riesgos, el diseño de seguridad no solamente debe estar pensado en la amenaza externa, sino que también se debe considerar la amenaza interna, quien en ultimas tiene

mayor facilidad para vulnerar y acceder a la información de la compañía; allí toman fuerza que todas las áreas deben estar sincronizadas en la confiabilidad de las personas, razón por la cual desde el proceso de selección, contratación, inducción y en las actividades diarias, se deben tener definidos los procedimientos a cumplir en la organización para poder filtrar a cada uno de los aspirantes como al personal ya contratado.

Siendo fundamental que los controles en el personal no solamente se realicen al momento de ingreso a la compañía, sino que por el contrario se esté realizando monitoreo a los comportamientos de las personas y de esta manera estar en capacidad de detectar comportamientos sospechosos que podrían afectar los intereses de la empresa.

La seguridad de la información se debe considerar como uno de los procesos más sensibles de una organización, por tanto no solamente con los controles tecnológicos se minimiza el riesgo, también se debe considera la confiabilidad de las personas que manipulan o diseñan los controles de seguridad, teniendo en cuenta que ellos podrían ser quienes vulneren los controles de seguridad y materializar cualquiera de los riesgos que se hayan identificado en el proceso de seguridad de la información.

Importancia de las Auditorias en seguridad

En términos del texto del autor “En la auditoria de seguridad, el desarrollo concreto de un programa de trabajo depende de las circunstancias particulares de cada empresa; se concentra en los riesgos y vulnerabilidades que pueda tener el sistema de gestión de seguridad y es definida como el examen o evaluación que se realiza utilizando técnicas para establecer en qué medida las

empresas logran sus objetivos, cumplen con los planes, programas y propósitos del Sistema de Seguridad. Así como la eficiencia, eficacia y economía en la gestión de los recursos destinados a la seguridad física e industrial de la empresa". (http/admejoresseguridad.com- ADMEJORES SEGURIDAD LTDA).

Más allá del buen diseño e implementación de un sistema de gestión en seguridad en una organización, se debe considerar claramente la puesta en marcha periódicamente de las auditorias en seguridad, las cuales son básicamente evaluaciones a los controles y poder determinar la eficacia y eficiencia de cada uno de los sistemas implementados, siendo en este proceso donde se permitirá tomar decisiones que le aporten a la mejora continua en la organización.

Al momento de planear una auditoria en seguridad, se debe considerar el conocimiento técnico que puedan tener las personas que van a realizar el ejercicio de auditoría, por tanto más allá de verificar si se cuentan con los recursos, es poder determinar que tanto se está preparado para una situación adversa, donde se integra inclusive el tema de la continuidad de los negocios y por consiguiente la importancia que toma cada vez más en las múltiples compañías a nivel mundial.

El realizar auditorías en seguridad, le permite a una organización, demostrar trazabilidad y seguimiento frente a un riesgo que se pueda materializar y adelantarse a dichos eventos de tal forma que mediante el tratamiento de los riesgos y la aplicación de planes de acción, se puede pensar en el futuro de cómo contrarrestar cualquier situación anómala y sobre todo contar con personal y procedimientos claros y expeditos, que faciliten la operación frente a los diferentes riesgos que puedan estar inmersos en la operación y el entorno en general.

A diferencia de unas pruebas de vulnerabilidad, el programa de auditoría en seguridad, no solamente evidencia fallas en el sistema, por el contrario, sensibiliza y busca mejoras efectivas, donde se pueden involucrar las pruebas de vulnerabilidad, de tal forma que toda la organización gire en torno a la mejora continua y las actividades de control se realicen por efecto de la cultura y no como una acción preventiva frente a una evaluación programada, por tanto es fundamental tener en cuenta que al momento de presentarse un siniestro, este no está planeado por la organización, por el contrario está plenamente analizado por el factor de amenaza que quiere causar daño sin ser detectado, vulnerando siempre los sistemas actuales de seguridad, por ende la necesidad de estar en gestión hacia la actualización de sistemas y mecanismos de control y seguridad.

¿Qué es un plan de continuidad de negocio?

Según lo manifiesta el autor "Un Plan de Continuidad de Negocio se compone de varias fases que comienzan con un análisis de los procesos que componen la organización. Este análisis servirá para priorizar qué procesos son críticos para el negocio y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción. (Laura del Pino Jiménez- 2007).

El plan de continuidad de negocio, es una de las actividades que ha alcanzado mayor fuerza en la gestión integral de riesgos, y que requiere del mayor análisis por parte de la gerencia

de la compañía, y en general todos los niveles de la compañía, por tanto toman parte activa para la ejecución y puesta en marcha en caso de presentarse alguna emergencia.

Los planes de continuidad de negocio (BCP), han experimentado un tema muy particular en las organizaciones contemporáneas: EL COSTO DE IMPLEMENTACION DEL BCP. Esta situación muchas veces obedece a ver la seguridad como un gasto mas no como una inversión, soportado en ocasiones en la cantidad de siniestros que han tenido, razón por la cual, siendo la seguridad de carácter preventivo, se visiona en muchas organizaciones reactivamente y solamente hasta que ocurren los siniestros se llega a la conciencia de la seguridad, realizando inversiones muy costosas para poder tratar de solucionar en el peor de los casos un intangible que afecta considerablemente la continuidad de los negocios: ¡la imagen!.

El poder trabajar y planear en las organizaciones las 3 fases de las emergencias: antes, durante y después, le permitirá prepararse y simular escenarios en los cuales la compañía podría afrontar situaciones adversas y colocar en práctica un plan de continuidad del negocio, es cual se debe estar actualizando en periodos de tiempo cortos, permitiendo que el personal identifique y asuma el rol correspondiente en el evento de materializarse un riesgo identificado en la organización.

BCP- (Business Continuity Plan). Plan de continuidad del negocio

De acuerdo a como lo manifiesta el autor "La información es uno de los activos más importantes para las organizaciones, donde los sistemas de información y disponibilidad de estos juegan un rol preponderante para la continuidad de un negocio, por lo cual las organizaciones

desarrollan e implementan lo que se conoce como BCP (Business Continuity Plan), con el objetivo de mantener la funcionalidad de una organización, a un nivel mínimo aceptable durante una contingencia. Esto implica que un BCP debe contemplar todas las medidas preventivas y de recuperación para cuando se produzca una contingencia que afecte al negocio" (Goodstein, L. & Timothy N. &Pfeiffer J. (1998) Planeación Estratégica Aplicada. ("N" ed.). País, editorial.)

La implementación de un plan de continuidad del negocio, tiene como particularidad tres tiempos esenciales para poder colocar en práctica, como lo son: el antes, durante y después, y este ultimo basado en la recuperación de la operación y activación del plan de continuidad del negocio, basado en la atención de las posibles contingencias que se presenten durante la presencia del siniestro.

Como lo manifiesta el autor, el BCP, debe contemplar todas las medidas preventivas; es allí donde se fundamente que el BCP, requiere de una excelente planeación y apoyo de las diferentes gerencias con recursos, para poder programar el personal, capacitarlo, formarlo, y sobre todo motivarlo en la participación activa del plan de continuidad del negocio.

El plan de continuidad de negocio como conjunto de estrategias.

De acuerdo a lo que se puede analizar en lo manifestado por el autor "El Plan de Continuidad de Negocio, no es más que un conjunto de estrategias, procedimientos preventivos y reactivos que permiten un rápido retorno a una situación normalizada, dicho conjunto de estrategias y procedimientos son creados para que la actividad de la institución se recupere en un nivel aceptable después de una interrupción no prevista de sus sistemas de información, y de la

situación normal de funcionamiento”(KotlerPhiilip. (2003). "Los 80 Conceptos Esenciales del Marketing de la A a la Z". ("N" ed.). País, editorial).

Cuando se habla de la continuidad del negocio, básicamente estamos comentando sobre las diversas estrategias se deben adoptar como organización de forma preventiva y reactiva, con miras a normalizar la operación y por consiguiente permitir que la compañía perdure en el tiempo, garantizando estabilidad a todos sus funcionarios y grupos de interés.

La situación más difícil del plan de continuidad del negocio, es la aceptación en muchos casos por parte de las altas gerencias a entender que es un tema gerencial y que requiere de un presupuesto para poder planear y prever cuáles serán las necesidades que se tendrán en caso de una novedad, no obstante en los últimos años ha ido ganando aceptación y aunque no con los recursos que se deberían tener, ya se está considerando como parte de las inversiones anuales y a las cuales se les debe prestar mayor atención.

La mayor resistencia que afronta el plan de continuidad del negocio, es la aceptación por parte de todas las empresas a ver este BCP, como una inversión mas no como un gasto, y sobre todo entender que la seguridad debe ser preventiva y no reactiva.

Posibles fallas en el Plan de continuidad de negocio,

Según Juan Gaspar Martínez, “El plan de Continuidad de Negocio, uno de los principales obstáculos con que se encuentran las organizaciones a la hora de iniciar la elaboración de un plan de continuidad de negocio estriba en la carencia de pautas claras con las que abordar un proyecto integral. La cuestión no está en que no existan metodologías o herramientas con que hacerlo, pero

quizás la dificultad radique no en su ausencia, sino en la mayor o menor facilidad de su empleo".(Juan Gaspar Martínez, El plan de Continuidad de Negocio, editor Díaz de Santos, 2006, ISBN 8479787783, paginas 224.)

Aquí un plan de continuidad de negocio, como es sabido requiere inicialmente de la concientización de las personas que hacen parte de la organización y para ello se requiere de todo el compromiso de la alta gerencia y a partir de allí dar inicio con un esquema de trabajo que permita realizar una evaluación de riesgo; un análisis del impacto del negocio el cual lleve a desarrollar estrategias de recuperación, basados en experiencias que puedan aportar; la capacidad para trabajar en equipo con la gerencia, personal de auditoría interna, profesionales de las áreas a implementar de los factores críticos y de esta manera poder utilizar herramientas que nos permita automatizar y al final ayude a minimizar aquellos inconvenientes con recursos propios de la organización, brindando soporte y confiabilidad. Para el desarrollo del BCP se requiere de objetivos que en su momento proporcionen un esquema de trabajo sencillo y práctico donde su secuencia y contenido permita al responsable del planeamiento su elaboración, planteamiento, comienzo y progreso del proyecto.

Plan de recuperación del negocio.

Según Jacqueline Chapman, "Un plan de recuperación del negocio no le protege de la competencia ni de las fuerzas del mercado, pero al prepararlo puede que se dé cuenta de cómo su negocio podría beneficiarse del desastre de un competidor y al revés, claro está. No tenga reparos de discutir su plan con otras organizaciones o con otros directivos. Se sorprenderá de cuantos no han hecho nada hasta ahora. En este tema la discusión e intercambio de ideas solo puede

ayudarle. No tiene por qué entrar en detalles o discutir información comercial confidencial para poder participar en un debate abierto sobre que podría ocurrir y que se debería hacer".
(Jacqueline Chapman 2002)

Tal como lo manifiesta el autor, un plan de recuperación del negocio, no le protege de la competencia, ni de las fuerzas del mercado; ante esta afirmación se puede determinar la importancia que tiene una efectiva planeación, prevención y puesta en marcha ante una situación adversa, es así como una compañía se puede medir y pensar en el futuro como organización, pues se tiene como ejemplo el siniestro presentado en las torres gemelas, en el cual prácticamente muchas empresas dejaron de existir, al no contar con un plan de recuperación del negocio y másaún cuando tenían como soporte de operación la torre contigua, donde jamás se llegó a pensar que podría pasar un acto terrorista como el presentado el 11 de septiembre, y a partir de allí toma fuerza los planes de continuidad del negocio para todas las empresas y gobiernos.

Siempre el plan de continuidad del negocio y el plan de recuperación del negocio, se fundamentan en pensar: ¿qué haría la empresa en caso de?, ¿cómo reaccionaría la empresa en caso de?, ¿quiénes reaccionarían en caso de?, ¿dónde se reanudaría la operación en caso de? ¿Cuál sería la inversión como empresa en caso de requerir activar su plan de recuperación del negocio?, entre otras preguntas que pueden surgir ante los posibles escenarios que se pueden presentar ante un siniestro, el cual al no estar proyectado, prácticamente se asume con todos sus efectos.

La continuidad de la Empresa Familiar

Según Joan Maria Amat"La empresa familiar se enfrenta a una serie de problemas que la hacen más vulnerables que la empresa no familiar. Sin embargo, aunque cada empresa familiar tiene sus propias características estos problemas son bastante previsibles y comunes. Por esta razón este texto presenta un conjunto de conceptos y modelos teóricos que complementa con el análisis de los problemas más importantes con los que se encuentran las empresas familiares y con los aspectos más relevantes de las empresas que tienen éxito y de las que fracasan.". (Joan Maria Amat, La Continuidad de la Empresa Familiar, Gestión 2000, 08034 Barcelona 176 páginas)

Tal como lo manifiesta el autor, en su libro donde generalmente los negocios de familia estaban identificados bajo tres círculos por varios autores y expertos en el tema, aquí se presenta un modelo donde son señalados cinco círculos que son considerados como críticos para las empresas familiares donde los problemas de cada una de las áreas se pueden identificar para darle mejor manejo y solución.

Las empresas familiares son organizaciones las cuales presentan características especiales respecto a las organizaciones convencionales, ya que el estar conformadas inicialmente por un modelo de tres círculos como la familia, la propiedad y el negocio los grandes autores y expertos en el tema dieron continuidad a sus estudios hasta llegar al modelo de cinco círculos donde el autor adiciona la gestión y la sucesión, aquí lo que se busca es lograr un diseño de estrategia de

gobierno que permita separar los temas relevantes de familia empresaria aquellas que puedan afectar la empresa familiar cubriendo del todo de una cosa a otra.

Siempre la continuidad del negocio dentro de sus círculos, la gestión, es considerada muy importante al tener que ver con aspectos relacionados con la organización, no solo de los recursos humanos sino tecnológicos y materiales, los cuales ayudaran a implementar el logro de objetivos estratégicos y mejorar la posición competitiva. La sucesión es considerada como el área de la planificación y gestión del proceso de traspaso si se puede llamar del bastón de mando a la siguiente generación para que ella se encargue de dar continuidad de la familia empresaria en la empresa familiar. Ya las áreas de familia, propiedad y negocio donde se complementa valores, actitudes y relaciones familiares, estructuras de poder, donde los grupos accionariales, la gestión del patrimonio y creación de valor hacen que fortalezca su junta, consejo accionista y administrativo.

Como enfrentar una crisis empresarial

Según Rene Deister“En la actualidad, las empresas en general están cada vez más propensas a sufrir una crisis y la mayoría no está preparada para enfrentar ese tipo de problemas. Las crisis corporativas llegan de improviso y ocasionan daños irreparables, por lo que es necesario que las empresas cuenten con un plan de respuesta inmediata y coordinada del más alto nivel. Esto implica designar un equipo responsable de las comunicaciones durante la crisis, manejar las relaciones con los medios de comunicación, definir y establecer los públicos internos y externos involucrados, definir los mensajes que se van a comunicar para cada caso e

implementar acciones y seguimiento”(Rene Deister, Como enfrentar una Crisis Empresarial, Editorial Trillas S.A. de C.V. México D.F.Edición febrero de 2008 112 páginas)

Cuando se habla de cómo enfrentar una crisis empresarial nunca se piensa que las empresas sean ajenas a caer en desgracia por diferentes razones encontrando a veces falta de compromiso de la alta Gerencia, donde se puede llegar a evidenciar la falta de toma de decisiones que son muchas veces reflejadas en el desconocimiento de empresarios que nunca llegan a contemplar que puede llegar a suceder.

Importante identificar indicadores y situaciones que pueda en su momento generar en la empresa que la crisis está por llegar de un momento a otro, por situaciones como la participación en el mercado, el nivel de ventas, el atraso de obligaciones, las amenazas de los acreedores, los préstamos extra bancarios para financiarse, el alto nivel de endeudamiento y los recortes de personal que deben realizarse.

Por eso dentro de otros tipos de crisis que una organización a que se ve enfrentada y debe ser considerada; son los fenómenos naturales como terremotos, incendios e inundaciones que puedan afectar las infraestructuras de los edificios, plantas, bodegas y otros; igualmente estas fallas pueden presentarse en la parte de tecnológica y para ello es necesario que toda organización tome las medidas para enfrentarlas, organizándose y preparándose a través de planes de contingencia donde sea identificados, analizados y evaluados los posibles riesgos, para su respectivo tratamiento conformando equipos de trabajo bajo el liderazgo de personas con capacidad de afrontarla

Manejo de Crisis durante una Contingencia

Según Paul Remy Oyague "Las crisis son eventos destructivos. Amenazan rápida y violentamente los márgenes financieros, la posición en el mercado, la reputación y hasta la continuidad del negocio. Nadie está libre de ellas. Una vez iniciadas, tienden a escalar agresivamente y expandir el daño. Hay que reaccionar de manera inmediata y actuar de modo coherente en una serie de ámbitos simultáneos" (Paul Remy Oyague, Manejo de Crisis, Editorial Universidad Peruana Ciencias Aplicadas UPC)

Como lo manifiesta el autor las crisis finalmente estallan, creando un poder destructivo, donde el daño está hecho y el problema creado siendo necesario actuar decididamente identificando la crisis, contenido de la crisis y lograr controlar el daño buscándole solución al problema.

Estas tareas no son fáciles de implementar, por eso si se está preparado se tendrá una estructura corporativa para el manejo de crisis, la cual es diseñada para asegurar a la alta gerencia el conocimiento oportuno de las situaciones o incidentes que pueden llegar a generar una crisis, facilitando la evaluación de sus posibles impactos en la organización, apoyando acciones de respuesta para el control y desarrollando estrategias para evitar, minimizar o mitigar sus efectos.

En principio en un plan de crisis es crear conciencia de que pueden derivar situaciones de emergencia, que pueden escalar en situaciones de crisis y que la prevención es la herramienta a usar, basada en análisis juiciosos de los riesgos; igualmente se crea y se desarrolla una estructura

para el manual de crisis con unos roles y responsabilidades claramente definidos, teniendo presente de proveer recursos que garanticen el cumplimiento de responsabilidades y lo soporten en los diferentes aspectos.

METODO

El método de consulta utilizado para la realización de este ensayo en LA SEGURIDAD FISICA Y SUS COMPONENTES COMO PARTE FUNDAMENTAL EN LA CONTINUIDAD DE LOS NEGOCIOS, se remite a la consulta y lectura de textos en seguridad mediante la utilización de libros, revistas y páginas de internet, analizando cada uno de los escritos, y de acuerdo al conocimiento adquirido por parte de los 2 estudiantes de la especialización, se realizó un análisis a cada párrafo y se plasmó el pensar profesional y respetuoso de cada uno.

Se espera que sea de gran aporte al desarrollo futuro de nuevos especialistas y profesionales de seguridad en la consulta de tan importante profesión.

CONCLUSIONES

Para una organización él no contar con un plan de continuidad del negocio, fundamentado en procedimientos, controles de seguridad física, ayudas tecnológicas, identificación y cuantificación de los riesgos, entre otros; le puede generar la desaparición en el tiempo de la empresa. Es por esta razón que la gestión de riesgos toma mayor fuerza cada día y requiere de personal altamente calificado, con unos conocimientos y habilidades para desarrollar e implementar metodologías que permitan medir, monitorear y tratar los diferentes riesgos que puedan estar presenten según las características de negocio de una organización y su entorno.

La identificación de los riesgos mediante el análisis de las amenazas, las vulnerabilidades, y el impacto que puede ocasionar a una compañía, la materialización de unos de los riesgos, debe estar basada en una metodología en riesgos que permita monitorear y determinar cuál es el plan de acción a seguir para minimizar los riesgos y mantenerlos en un estado de control donde no afecte a la organización.

REFERENCIAS

- (Mary Lynn García. 2008), El Diseño y evaluación de los sistemas de protección física- (traducción al español- 2011). 15- 05- 12
- (Philip p. purpura. Purpura. 2002). 15- 05-12
- (Norma ISO 28000 – 2007). 20- 05-12
- (http://www.sisteseg.com/fisica.html). 4 -06- 12
- ([http://www.monografias.com/] boletín 27 Universidad EAFIT. Medellín). 4- 06- 12
- ((1) HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open PublicationLicense v.10 o Later. 2 de Octubre de 2000. 12-06-12
- (http://www.kriptopolis.org-) 15-06-12

  Escuela Universitaria de Informática -Universidad Politécnica de Madrid
- (http/admejoresseguridad.com- ADMEJORES SEGURIDAD LTDA-) 20- 06- 12
- (Laura del Pino Jiménez- 2007). 20- 06 12
- (Goodstein, L. & Timothy N. &Pfeiffer J. (1998) Planeación Estratégica Aplicada. ("N" ed.). País, editorial.) 4- 07-12
- (KotlerPhiilip. (2003). "Los 80 Conceptos Esenciales del Marketing de la A a la Z". ("N" ed.). País, editorial). 4- 07 12
- (Juan Gaspar Martínez, El plan de Continuidad de Negocio, editor Díaz de Santos, 2006, ISBN 8479787783, paginas 224.) 5- 07 12
- Jacqueline Chapman 2002, Plan de Recuperación de negocios en una semana. Traducción Enric Barba, ediciones Gestión 2000, Planta De Agostini profesional y formación, SL Barcelona, 2006. 4- 07-12

- Normas APA (2009, 28 de marzo). Recuperado el 30 de marzo de 2011 de http://www.slideshare.net/rchoquel/normas-apa-1430826
- Seguridad ATLAS LTDA- ADMIRA- 2012- http//www.Atlas.com.co. – 4- 06- 12
- Joan Maria Amat, La Continuidad de la Empresa Familiar, Gestión 2000, 08034 Barcelona 176 páginas.
- René Deister, Como enfrentar una Crisis Empresarial, Editorial Trillas S.A. de C.V. México D.F. Edición febrero de 2008 112 páginas.
- Paul Remy Oyague, Manejo de Crisis, Editorial Universidad Peruana Ciencias Aplicadas UPC
- José Luengas, CPP, DSI Manejo de crisis durante una contingencia, consultoría manejo de crisis. Crisiscontrol.com.mx – mx.linkedin.com